EXHIBIT A

U.S. AGENCY FOR GLOBAL MEDIA | UNITED STATES BROADCASTING BOARD OF GOVERNORS

330 Independence Avenue SW | Washington, DC 20237 | usagm.gov

April 3, 2020

The Honorable Lindsay Graham
Chairman
Subcommittee on State, Foreign Operations and Related Programs
Committee on Appropriations
United States Senate

Dear Mr. Chairman:

The U.S. Agency for Global Media (USAGM) hereby submits this report, pursuant to Section 7050(b) of the Further Consolidated Appropriations Act, 2020 (Div. G, P.L. 116-94). It is the agency's plan for programs to promote Internet freedom globally, including a description of safeguards to help ensure that such programs are not used for illicit purposes.

Should you have any questions please contact Adam Tracy, Congressional Liaison, at 202-203-4669.

Sincerely,

Grant K. Turner

Grant K. Turner
Chief Executive Officer and Director

Enclosure

# U.S. Agency for Global Media
# Internet Freedom FY 2020 Spend Plan

| Managing Network | FY 2018 IF Actual | FY 2019 IF Actual | FY 2020 IF Projected |
|---|---|---|---|
| USAGM/OIF | 4,300,000 | 5,298,770 | 175,000 |
| RFA/OTF | 10,700,000 | 9,701,230 | 1,200,000 |
| OTF, Inc. | 0 | 0 | 19,825,000 |
| **Total** | **15,000,000** | **15,000,000** | **21,200,000** |

Pursuant to the Further Consolidated Appropriation Act, 2020, P.L. 116-94 (FY20 Appropriation Act) the Agency was provided $20,000,000 in no-year funds which shall be for internet freedom (IF) programs. This spend plan details the USAGM's Office of Internet Freedom (OIF) and the Open Technology Fund's (OTF) priorities and operations for these FY 2020 funds. The plan is submitted in compliance with section 7050(b) of the FY20 Appropriation Act, and as may be applicable, section 7015 and 7061 of that Act.

The mission of the United States Agency for Global Media is to "inform, engage, and connect people around the world in support of freedom and democracy." In furtherance of this mission, USAGM has been supporting internet freedom projects since 2012 through the Office of Internet Freedom (formerly the Internet Anti-Censorship Division) and the Open Technology Fund (OTF), USAGM's newest non-profit grantee. The USAGM's internet freedom program supports, per congressional appropriations guidance, global internet freedom for the expansion of unrestricted access to information on the internet. Over the past seven years, USAGM has invested over $100 million in projects to promote internet freedom in the world's most restricted environments. Together, these programs have supported the tools and techniques necessary for USAGM networks to report and disseminate content in information-restrictive markets, and for USAGM audiences to receive and share content safely online.

USAGM's target audiences across the world increasingly access media content via digital and social media platforms. In 2019, USAGM's unduplicated digital audience reached 127 million people, representing a 22% growth from the previous year. In parallel, threats to internet freedom have escalated dramatically. Repressive regimes are deploying a new generation of advanced censorship and surveillance technology that is designed to stifle dissent, track minorities, and manipulate content online. China alone spends billions of dollars each year to maintain its complex censorship and surveillance apparatus, while Russia and Iran are each investing hundreds of millions of dollars to build what are fundamentally "national intranets." These and other efforts by repressive regimes are fundamentally re-shaping the internet from a shared, global platform to isolated networks of censorship and control. Today, over two thirds of the world's population live in countries where the internet access is restricted, and that number is growing. This makes it difficult and dangerous for USAGM journalists, sources, and audiences to engage in and share fact-based news online.

Technologies that provide access to blocked content, and safe and secure methods to share content, are critically important to getting information to target audiences that would otherwise be siloed by government censorship. USAGM's IF program enables not only unfettered online access to USAGM products or content, but also the full spectrum of independent news sources on the internet. This is increasingly important as the USAGM continues to harness digital platforms and undertakes new methods of engaging with audiences. Accordingly, projects focused on safe and secure communications are critical components for ensuring that the USAGM content creation process does not expose our stringers, sources, and interviewees to threats, and that USAGM news and information is delivered to these audiences without further endangering them. Addressing the online threats faced by USAGM's audiences and protecting journalists, sources, and information seekers against punishment for online activity are essential to fostering free media, and necessitate deploying tools that both circumvent censorship and protect user access to information.

In response to escalating attacks on freedom of expression, USAGM, with congressional support, established the Open Technology Fund as USAGM-sponsored independent organization. This allows for the consolidation of previous streams of effort into a synchronized and expanded capacity to protect internet freedom around the globe.

USAGM's FY 2020 budget provides $20 million to the International Broadcasting Bureau for internet freedom programs, and $1.2 million to RFA for associated staffing costs to continue support services as OTF builds out an administrative team. As detailed above, of the $21,200,000 allocated for internet freedom programs, USAGM will provide $19,875,000 to the newly established Open Technology Fund corporation through a grant agreement and will hold back $175,000 for the Office of Internet Freedom to support OIF's oversight activities, including monitoring and evaluation efforts.

Radio Free Asia (RFA) has engaged the services of its auditors, Calibre CPA Group to review the open contracts on RFA's financial records as of May 31, 2020. Upon completion of this review, any unobligated and obligated funding, along with any unused portion of the $1.2 million for associated staffing costs during the transition will be transferred to OTF. The estimated completion of this review is mid-June.

## OFFICE OF INTERNET FREEDOM

Since 2002, USAGM has been involved in activities to circumvent internet censorship by foreign governments in order to distribute news content and better provide a forum for free expression in closed countries. In 2016, USAGM established the Office of Internet Freedom (OIF) to conduct governance and oversight of USAGM internet freedom activities.

OIF no longer directly implements or manages internet freedom projects or contracts but rather will manage projects that assess particular threats and/or OTF effectiveness in appropriate areas to inform USAGM strategy and oversight. The Open Technology Fund, a non-federal entity, will implement the internet freedom program in full, including support for all USAGM news networks. More details about this transition are included later in the OTF section below.

OIF will continue to perform critical oversight to ensure OTF compliance with relevant rules and regulations in the execution of congressionally mandated use of internet freedom funds for technology projects, ensuring uninterrupted circumvention services for USAGM entities and their training needs. The Director of the OIF, currently the sole employee assigned to OIF, will participate in the OTF proposal review process as a member of the OTF Advisory Council and have full access to the proposal vetting lifecycle.

| OFFICE OF INTERNET FREEDOM<br>SPEND PLAN<br>FY 2020 | | |
|---|---|---|
| Third party evaluation of circumvention tools at scale | $100,000 | 57.5% |
| Research reports on the reach of OTF-incubated projects | $50,000 | 28.5% |
| Programmatic support | $25,000 | 14% |
| **GRAND TOTAL, OIF** | **$175,000** | **100%** |

## OPEN TECHNOLOGY FUND

Since its creation in 2012, the Open Technology Fund has been incubated by Radio Free Asia, a non-profit USAGM-sponsored grantee. During this time, OTF has supported pioneering research, development, and implementation of cutting-edge internet freedom technologies to respond to rapidly evolving censorship threats around the world. Today, over two billion people globally use OTF-supported technology daily, and more than two-thirds of all mobile users have OTF-incubated technology on their device.

In September 2019, OTF was incorporated as an independent non-profit organization. The creation of an independent Open Technology Fund enables USAGM to further build on its success, expanding its internet freedom efforts and maximizing the impact of its investments. With a growing percentage of USAGM's audiences relying on the internet to access news and information, it is essential that they have the tools necessary to do so safely, and free from censorship and surveillance. The same is true of USAGM journalists, stringers, and sources who are constantly exposed to threats throughout the reporting process.

As an independent organization, OTF is uniquely situated to responsibly and accountably support the U.S. government's internet freedom efforts at the pace and with the flexibility needed to empower innovation and compete against adversaries to a free and open internet. These additional resources will enable OTF to increase long-term support for core internet freedom tools, expand funding for next generation solutions, and provide direct technical and digital security support to USAGM networks.

## MISSION

The Open Technology Fund works to advance internet freedom in repressive environments by supporting the applied research, development, implementation, and maintenance of technologies that provide secure and uncensored access to USAGM's content and the broader internet to counter attempts by authoritarian governments to control the internet and restrict freedom online, including secure communications between journalists and sources.

Historically, OTF has supported the research, development, and implementation of cutting-edge internet freedom technologies. As an independent organization, OTF's mission has expanded to support a broader range of technologies to respond to increasingly aggressive and sophisticated censorship and surveillance threats and to provide more comprehensive and tailored support to USAGM networks. OTF will continue to work to advance internet freedom globally but, in addition to supporting the research, development, and implementation of innovative internet freedom technologies, OTF will also support the long-term maintenance and advancement of core internet freedom tools. This will enable OTF to provide tailored support throughout the entire technology development cycle from proof-of-concept, to on-the-ground deployments, to multi-year efforts to better support technology development at speed and scale. Additionally, OTF will provide direct internet freedom assistance to USAGM's news networks to improve the digital security of USAGM entities and journalists, including making USAGM websites and applications more secure and resistant to censorship, providing customized and secure tip lines for sources, and deploying leading internet freedom technologies to ensure that audiences can access USAGM content despite increasing censorship. This expanded support will ensure that USAGM journalists and audiences have the tools they need to safely access the uncensored internet today as well as respond to future censorship threats.

## OBJECTIVES

Consistent with section 7050(b) of the Further Consolidated Appropriations Act, 2020 (P.L. 116-94), to "carry out research and development of new tools or techniques" and "utilize tools and techniques to securely develop and distribute USAGM digital content", OTF supports programs to:

- **Provide uncensored access to the internet** to individuals living in information-restrictive countries to ensure that they can safely access USAGM content. This entails the development and deployment of circumvention technology as well as research and awareness-raising that help circumvention technology stay a step ahead of the censors.

- **Protect journalists, sources, and audiences** from repressive surveillance and digital attacks to ensure that they can safely create and consume USAGM content. This includes support for secure communication tools, targeted digital security interventions and other forms of privacy and security technology.

## OTF PROGRAMS

OTF solicits project ideas through a fully open and competitive application process. The OTF application process has been designed to reduce barriers to entry to make funding more accessible to a wide scope of qualified individuals and organizations around the world. This process has helped to attract innovative applications from groups that are not typically able to access federal funds, including expert technologists, frontline journalists and human rights defenders, cutting-edge researchers, and digital security specialists. In order to ensure a high degree of due diligence during the application review process, OTF implements a multi-stage process through which successful applications are improved and refined to maximize impact. Through this process all proposals are reviewed by OTF experts as well as OTF's all-volunteer Advisory Council, a group of nearly 40 technical, regional, and subject-matter experts from a wide range of relevant disciplines, who provide feedback, guidance, and rankings for all proposals. In addition to ensuring that the most competitive and impactful projects are funded, this multistage review process also achieves substantial cost savings.

In order to fully support the technology development cycle, OTF provides resources through a variety of implementation mechanisms to enable tailored and comprehensive support to internet freedom projects. Because internet censorship technology and tactics are constantly evolving and adapting, OTF receives, reviews, and contracts projects on a continual rolling basis.

- **Funds:** OTF provides direct funding to support the applied research, development, implementation, and maintenance of technologies that enable censorship circumvention and enhance user security and privacy online.

  - **Internet Freedom Fund (IFF)** is the primary mechanism through which OTF provides funding for innovative global internet freedom projects. IFF projects are primarily focused on technology development and implementation but can also include applied research and digital security projects. Through an open and competitive process, OTF solicits project proposals to the IFF every two months. Projects funded through the IFF typically range from $10,000 - $500,000. OTF anticipates supporting 75-90 projects with these FY 2020 resources. **(Projected FY20 budget: $7,000,000)**

  - ○ **Technology at Scale Fund** is the means through which OTF supports the circumvention and secure communication technology needs of USAGM networks. The fund will solicit technology solutions to deliver USAGM content to audiences in information-restricted environments and protect USAGM journalists and sources. It will also ensure that technologies already used at scale by millions remain secure and effective. Projects funded through the Technology at Scale Fund will range from $500,000 - $2,500,000. OTF anticipates supporting 6-8 large-scale technologies that have a proven track record of successfully and safely circumventing online censorship in highly internet restricted environments and/or providing secure content sharing and communications in repressive contexts with these FY 2020 resources. **(Projected FY20 budget: $7,000,000)**

  - ○ **Core Infrastructure Fund** supports the core infrastructure of everyday internet freedom technology to ensure the resiliency of digital security and circumvention tools. This infrastructure, such as PGP, SSL, SSH, OTR, SNI, TLS, pluggable transports and code libraries, is utilized by people throughout the world to increase their access, privacy and security online. Supporting these efforts is essential to ensuring the efficacy and security of critical circumvention and security tools. OTF anticipates supporting 6-8 projects with these FY 2020 resources. **(Projected FY20 Spend: $750,000)**

  - ○ **Prototype Fund** supports the rapid development of cutting-edge internet freedom technology prototypes that serve the immediate needs of independent journalists and human rights defenders. Through this fund, technologists and activists receive support to bring to life next-generation solutions that address emerging censorship and surveillance threats. Projects funded through the Prototype Fund range from $3,000 - $6,000. OTF anticipates supporting 10-20 projects with these FY 2020 resources. **(Projected FY20 budget: $70,000)**

  - ○ **Rapid Response Fund** provides emergency support to independent media outlets, journalists, and human rights defenders who face digital attacks to help them stay safe, get back online and mitigate future attacks or to combat sudden censorship events. OTF will have the capacity to support at least 20 rapid response engagements with these FY 2020 resources. **(Projected FY20 budget: $500,000)**

- **Labs:** In addition to direct funding, OTF provides expert services to the internet freedom community at large through its Labs, including security code audits, usability assessments, engineering support, the translation and localization of internet freedom tools into over 200 languages, legal information and referrals for pro-bono legal support, and secure cloud storage. These services fall under six labs: the Engineering Lab, the Red Team Lab, the Usability Lab, the Community Lab, the Localization Lab, the Learning Lab and the Legal Lab.

  These services also ensure that the technologies incubated and supported by OTF are as effective, secure, and usable for USAGM audiences as possible. By coordinating the provision of these services through the labs, OTF is able to achieve large economies of scale and bring down the overall cost of providing expert support to internet freedom projects. These services are available to both OTF-funded projects, as well as other important internet freedom efforts, through applications associated with each lab. These FY 2020 resources will allow OTF to scale up its Lab services to fully support the programs described above. **(Projected FY20 budget: $1,775,000)**

- **Research Fellowships:** OTF supports individuals to carry out cutting-edge applied research projects examining how authoritarian states are restricting the free flow of information and ways for citizens to overcome those tactics. OTF fellowships help to cultivate the next generation of internet freedom experts by creating a viable career track for those who have the skills and passion for internet freedom. Over the course of the last six rounds of fellows, the program has both (a) produced extremely timely and impactful breakthroughs that immediately feedback into the development of internet freedom technologies, and (b) received applications from some of the most highly-regarded researchers and technologists who take leave from high profile and highly paid positions in order to focus on a particularly important area of research. The cost per fellowship averages $60,000 and OTF anticipates supporting 10-12 fellows with these FY 2020 resources. **(Projected FY20 budget: $500,000)**

- **Entity Support Program:** Evolving an effort launched by OIF in FY 2019, OTF will hire expert digital security consultants to provide direct internet freedom assistance to USAGM networks, such as technical audits and digital security trainings, to improve the digital security of its entities and journalists. Based on findings of these digital security interventions, OTF will leverage resources available through its other funding mechanisms to support the entities ongoing internet freedom needs, such as making USAGM websites and applications more secure and resistant to censorship, providing customized and secure tip lines for sources, and deploying leading internet freedom technologies to ensure that our audiences can access USAGM content despite increasing censorship. These FY 2020 resources will enable OTF to begin piloting the Entity Support Program with Radio Free Europe/Radio Liberty and Voice of America. **(Projected FY20 budget: $260,000)**

- **OTF Summit:** Since its inception, the OTF Summit has been an annual retreat for invited OTF projects, fellows, advisory council members and other experts in the field (including public and private funders) to focus on OTF program review/assessment, landscaping the state of play on internet freedom in hot spots around the world, setting priorities for the coming year, strengthening collaboration, and growing the impact of the IF community. This ensures that OTF remains deeply integrated with the latest developments in censorship and surveillance technology and tactics in the field as well as emerging breakthroughs to counter threats to internet freedom. **(Projected FY20 budget: $200,000)**

- **OTF Program Support:** In addition, funding is set aside for OTF Program Support including, but not limited to: training, travel for project monitoring, participating in industry conferences as necessary to address emerging threats, collaborations with complementary programs, infrastructure, proposal system maintenance and other costs for making the programs run effectively, efficiently and collaboratively. **(Projected**

**FY20 budget: $350,000)**

- **One-time Start-up Costs:** OTF anticipates the following one-time start-up expenses to establish a fully independent organization: office space, supplies, expansion of OTF's proposal system in incorporate back-end functions such as invoicing and contract management, start-up service fees for accounting, payroll, human resources. **(Projected FY20 budget: $500,000)**

- **Salaries and Operations:** This covers the cost of OTF staff, fringe, office space, and other general direct costs. More details about OTF staffing and leadership are provided below. **(Projected FY20 budget: $2,120,000)**

| **OPEN TECHNOLOGY FUND<br>SPEND PLAN<br>FY 2020** | | |
|---|---|---:|
| Internet Freedom Fund | $7,000,000 | 33% |
| Technology at Scale Fund | $7,000,000 | 33% |
| Core Infrastructure Fund | $750,000 | 3.5% |
| Prototype Fund | $70,000 | 0.5% |
| Rapid Response Fund | $500,000 | 2.5% |
| OTF Labs | $1,775,000 | 9% |
| Research Fellowships | $500,000 | 2.5% |
| USAGM Entity Support | $260,000 | 1% |
| OTF Summit | $200,000 | 1% |
| Programmatic Support | $350,000 | 1.5% |
| One-time start-up costs | $500,000 | 2.5% |
| **OTF Programmatic and Operations Subtotal** | **$18,905,000** | **90%** |
| OTF Staff | $2,120,000 | 10% |
| **OTF Staff Subtotal** | **$2,120,000** | **10%** |
| **GRAND TOTAL, OTF** | **$21,025,000** | **100%** |

## OTF OPERATIONS

### Leadership

OTF will have both a CEO and President to fully and efficiently support the creation of the organization.

Libby Liu is the inaugural CEO of the OTF grantee corporation. Prior to joining OTF, Ms. Liu was the President of RFA for nearly 20 years, where she provided the private non-profit grantee with leadership, vision, and mission-based strategic and operational direction. Under Ms. Liu's leadership, RFA transformed from a radio broadcaster to a wholly digital multi-media interactive news organization. Ms. Liu also created OTF as a program within RFA in 2012 and has overseen OTF as a program at RFA for the past seven years.[1]

The CEO is responsible for leading the start-up of the OTF grantee and establishing the organization including financial, legal and HR infrastructure. The CEO will also lead OTF's development strategy, including external relations, partnerships, fundraising, and serve as the primary liaison to the OTF Board. The CEO will also serve as a member of USAGM Internal Coordinating Committee. The CEO position is expected to be a short-term role to lead the initial start-up and establishment of the OTF corporation. At the conclusion of the CEO's term, the CEO and President roles will be collapsed into a single position, consistent with other USAGM entity leadership structures.

Laura Cunningham is the inaugural President of the OTF grantee corporation. As President, Ms. Cunningham is responsible for OTF's strategic development, long-term planning, and day-to-day operations to enable OTF to fulfill its mission to support internet freedom worldwide. Ms. Cunningham has over a decade of experience working on internet freedom across a variety of donor, non-profit, and government organizations. Prior to joining OTF, Ms. Cunningham was the Senior Advisor for Internet Freedom in the U.S. State Department's Bureau of Democracy, Human Rights and Labor, where she led the Department's internet freedom programs focused on technology development, digital security, internet policy advocacy, and research.[2]

[1] Prior to joining RFA, Ms. Liu served as the Director of Administration and Strategic Planning at the Baltimore headquarters of the National Association for the Advancement of Colored People (NAACP). There she played a pivotal role in the Board's establishment of the NAACP's Five-Year Strategic Plan Goals and Objectives and in the implementation of the Plan. Ms. Liu holds a bachelor's degree from the University of California-Berkeley, an MBA from the Wharton School at the University of Pennsylvania and a JD from the University of Pennsylvania Law School.

[2] Prior to joining the State Department, Laura was Program Manager of ICT Policy and Programs at Internews. Previously, Laura worked as a Digital Coordinator at the Center for International Media Assistance at the National Endowment for Democracy, and helped to launch the Liberation Technology Program at Stanford University's Center for Democracy, Development and the Rule of Law. Laura holds an M.A. in comparative politics and a B.A. in political science, with a minor in computer science, from Stanford University.

## OTF Board

Per USAGM policy, all USAGM Board members were offered the opportunity to participate on the OTF Board and all six Board members opted in, including Mr. Kenneth Weinstein, as Board Chairman, Dr. Leon Aron, Ambassador Ryan Crocker, Mr. Michael Kempner, Ambassador Karen Kornbluh, and the Secretary of State, ex officio, or his designee.

Given the highly technical nature of OTF's work, the OTF Board has the ability to add additional experts to the Board. To date, the Board has added Ben Scott to the Board. Mr. Scott is Director of Policy & Advocacy at Luminate. Prior to joining Luminate, he co-led the Stiftung Neue Verantwortung (SNV) in Berlin, where he helped to develop it into a leading tech policy voice in German politics. He also was a senior adviser to a think tank in Washington DC, where he helped design the Public Interest Technology Initiative. Previously, Ben was Policy Adviser for Innovation at the U.S. Department of State, where he helped steward the 21st Century Statecraft agenda, with a focus on technology policy, social media, and development. Before this, Ben led the Washington office of Free Press, a public interest organization expanding affordable access to an open internet and fostering more public service journalism.

## Staffing

The OTF team currently consists of twelve full-time team members: one CEO, one President, one Deputy Director, one Director of Technology, one General Counsel, one Director of Research, one Director of Digital Security, three program managers, one program specialist, and one communications/social media outreach coordinator. As a whole, the team is rich with experience in the field of internet freedom. OTF's program managers include technical and implementation experts with deep knowledge of the regions where OTF's efforts are most needed. OTF's technical experts are developers, computer science experts, and digital security trainers/auditors. OTF's implementation experts have led technology and digital security initiatives for independent media outlets and human rights organizations around the world. OTF is in the process of hiring several additional staff members over the next year to fully support OTF operations, including human resources, external relations, finance and accounting experts, administrative and program staff.

## Monitoring and Evaluation

Monitoring and evaluating the success of OTF projects is key to OTF's ability to make informed, impactful and cost-effective funding decisions. Evaluation of OTF project success is conducted in accordance with the USAGM's Internet Freedom Framework. While projects vary in their individual metrics, all OTF-funded projects must clearly define an intended impact and present metrics for measuring success as part of the OTF application process. Moreover, the vast majority of OTF contracts are constructed as pay-for-performance, which is only possible with the hands-on program management central to the OTF approach. Metrics for each project are approved by the OTF team and reported to the Director of the Office of Internet Freedom in the Office of the Chief Strategy Officer.

## Mitigating Illicit Use

OTF engages in internet freedom activities with the goal of expanding the ability of individuals to exercise their fundamental freedoms – including rights to freedom of expression, association, and peaceful assembly – for peaceful and democratic ends. Internet freedom programming, by its nature, presents new challenges and opportunities for mitigating restrictions on the exercise of fundamental freedoms online. As with any technology, including a laptop computer or a cellular telephone, there is no absolute way to ensure that the products developed through USAGM internet freedom programs are not used for illicit ends; however, OTF implements a comprehensive illicit use mitigation strategy to minimize the potential for illicit use of supported technologies to the greatest extent possible. OTF carefully considers risk factors in its review process and programming efforts and performs due diligence and risk assessments on grantees prior to the issuance of awards. Additionally, the design and deployment of OTF-supported internet freedom technologies are geared towards repressive environments; they are designed specifically to meet the needs of independent journalists, information seekers, human rights defenders and other at-risk user groups in societies where speech is severely restricted; and distribution methods and networks for internet freedom technologies focus on helping individuals in internet-repressive environments. OTF re-evaluates its illicit use review process and mitigation strategy on an ongoing basis to ensure it remains relevant and effective. OTF is currently coordinating with the internet freedom program at the State Department's Bureau of Democracy, Human Rights and Labor to commission such a re-evaluation.

## OVERSIGHT

USAGM will continue to provide oversight of all OTF activities. Overall oversight responsibility will be led by the USAGM's CEO while OTF's programmatic work will be overseen directly by USAGM's Director for the Office of Internet Freedom in the Office of the Chief Strategy Officer, and OTF's budget and finances will be overseen by USAGM's Budget Office. In order to ensure USAGM has full transparency over OTF's operations and is able to provide appropriate oversight, OTF will provide USAGM with an annual spend plan, monthly programmatic and financial reports, and an annual report on OTF's annual illicit use mitigation strategy as well as other reviews and reports upon request.

In addition to USAGM oversight, OTF is committed to meeting all Congressional oversight requirements and requests, including the timely preparation of the annual USAGM Internet Freedom Spend Plan.

## COORDINATION WITH USG FUNDERS

OTF is committed to maintaining and expanding strong partnership and close collaboration with all other USG internet freedom funders to share information, identify opportunities for complementary work, avoid duplicating efforts and leverage efficiencies. OTF works closely with the U.S. Department of State's Bureaus for Democracy, Human Rights, and Labor (State/DRL) and Near Eastern Affairs (State/NEA), USAID's Bureau for Democracy, Conflict and Humanitarian Assistance, Center of Excellence on Democracy, Human Rights, and Governance (USAID/DCHA/DRG), and the Defense Advanced Research Projects Agency (DARPA). Each of these publicly funded internet freedom efforts participate in regular meetings and is active on online discussion groups to expand beyond the regular in-person meetings. Risk of funding duplication is low because each funder pursues a complementary approach and coordinates closely at both the program review level and throughout the project implementation period. In cases where potential overlap could occur, these funders have and will continue to avoid duplication by de-conflicting budgets at line item level detail, if necessary. Moreover, OTF and the State Department internet freedom program actively participate in each other's project review panels. As such, the impact and success of each program must be considered within the overall context of complementary strategies and portfolios reflecting the shared legislative goals and objectives. OTF staff also actively collaborates with relevant programs within the Federal Government increasing the ability to leverage existing funding streams. These programs include the Secure and Trustworthy Cyberspace at the National Science Foundation, the Science & Technology Cyber Security Division at the Department of Homeland Security, the U.S. Naval Research Laboratory and the Computer Security Division at the National Institute of Standards and Technology.

## LEVERAGING PRIVATE FUNDING

The annual Global Internet Freedom appropriations states that, "funds made available pursuant to this section shall be matched, to the maximum extent practicable, by sources other than the United States Government, including from the private sector." In pursuit of this goal, OTF has worked to educate private donors about internet freedom and encouraged them to increase funding for internet freedom initiatives. As a result of these efforts, leading private donors, including the Ford Foundation, the Hewlett Foundation, and the Media Democracy Fund, have made internet freedom a core component of their funding strategy and have invested millions of dollars to support internet freedom globally - many times in joint funding with OTF. In addition, OTF has actively engaged with the private sector and advocated for companies to adopt, integrate, and support internet freedom technologies. For example, due to OTF engagement, WhatsApp integrated the OTF-funded Signal protocol into the WhatsApp application, which now secures the communication of over 1.5 billion users worldwide.

As an independent organization, OTF will continue to engage private donors and encourage the private sector to increase funding and support for internet freedom tools and technologies. OTF will also continue to educate donors about the current Internet freedom landscape to help them best direct new resources. In addition, to these awareness-raising efforts, OTF will also work to leverage private funding through direct fundraising efforts. OTF's fundraising efforts will aim to unlock resources from private donors and the private sector that complement ongoing Congressional appropriations and fill critical internet freedom funding gaps. Per the nature of grant law and regulation and the required USAGM oversight over OTF operations, OTF will not engage in fundraising from other sources except in accordance with established USAGM policy. In addition, OTF will not use any Federal funds to finance its fundraising efforts, unless authorized by USAGM and in accordance with relevant laws and regulations.

## RECENT ACCOMPLISHMENTS

Threats to internet freedom have escalated dramatically in recent years.  Repressive regimes are deploying a new generation of advanced censorship and surveillance technology that is designed to stifle dissent, track minorities, and manipulate content online. China alone spends billions of dollars each year to maintain its complex censorship and surveillance apparatus, while Russia and Iran are each investing hundreds of millions of dollars to build what are fundamentally "national intranets." These and other efforts by repressive regimes are fundamentally re-shaping the internet from a shared, global platform to isolated networks of censorship and control. As a result, today, over two thirds of the world's population live in a country where the internet access is restricted, and that number is growing. This daily suppression of freedom of expression stifles the fundamental human rights of all citizens and prevents the development of open societies.

In response to these growing threats, over the last year, OTF funded over **60 innovative technology projects** to combat censorship and repressive surveillance, **22 fellowships** to support cutting-edge research and digital security interventions, **7 labs** to improve the security, usability, resiliency and interoperability of key internet freedom technologies, and over **50 rapid response interventions** to address digital emergencies.

**Technology to Fight Censorship and Repressive Surveillance**

Over the last year, OTF supported the development and implementation of cutting-edge technologies to fight increasingly sophisticated censorship and surveillance threats, including:

- **Advanced VPN Technology:** Virtual Private Networks (VPNs) have become one of the most popular methods for circumventing government-imposed censorship and, as a result, have become the target of repressive governments. Unfortunately, many popular, propriety VPNs rely on underlying protocols that have numerous, widely known vulnerabilities, massive codebases, and significant performance issues. In order to meet the demand for more secure, resilient, easy-to-use VPNs, OTF has invested in better documenting the vulnerabilities in widely used VPN protocols and the privacy practices of commercial VPNs and several emerging VPN solutions, such as Wireguard. Wireguard features a lightweight codebase, extensive security review, and integration of many important security features lacking in previous VPN protocols such as a "fail-closed" feature, which forces a more secure connection by default.

- **Emerging Circumvention Techniques:** The Chinese government constantly updates the Great Firewall (GFW) to prevent Chinese citizens from using new circumvention techniques to access blocked content. This process of updates creates a perpetual cat-and-mouse game between Chinese censors and new circumvention techniques. In response, OTF has supported the creation of an entirely new subfield of circumvention research that relies on machine learning techniques to constantly analyze the GFW. Through this analysis, researchers have discovered four new "species" of circumvention techniques and more than 25 distinct ways to overcome the GFW. These newly discovered techniques can rapidly evolve based on any changes made to the GFW and attempting to plug these holes in the GFW will in some cases open up new ones. The most promising mobile-friendly techniques are being pursued and developed into software kits for integration by circumvention tools. The researchers are also investigating techniques that will allow a content publisher to transmit information in ways that overcome the GFW and will allow users to access blocked content by simply pulling up the website on a browser.

- **Encrypted SNI:** Blocking websites through the unencrypted SNI field is an increasingly pervasive censorship tactic. This method of censorship is being used extensively in China as well as in Venezuela, which OTF-supported researchers discovered last year. Simply encrypting the SNI field would prevent censors from using this form of blocking. However, in order to encrypt SNI, browsers and website hosting providers must adopt this approach, which many have not because of a lack of standardization and difficulties related to implementation. Over the last year, OTF has supported a central actor in the IETF working group to finalize the encrypted SNI standard and create the template code to minimize any challenges associated with implementation. This will dramatically increase adoption of encrypted SNI and remove a primary blocking strategy employed by censorship regimes.

- **Secure Document Sharing and Storage:** As part of their daily operations, journalists, media networks, and human rights organizations frequently collect, store, and share sensitive information. This information often contains multiple layers of sensitivity and requires varying forms of protection from governments that seek to surveil and censor their citizens. In order to address this threat and to protect information at rest and shared within an organization, OTF has supported the development of several open source, secure file storage and file-sharing systems designed for journalists and human rights organizations, including Globaleaks, Tahoe-LAFS, OpenArchive, and OpenAppStack.

- **Mobile Surveillance Detection:** An international mobile subscriber identity-catcher (IMSI-catcher) is a surveillance device used to intercept mobile phone traffic and track mobile phone users. Over the last several years, repressive regimes have increasingly deployed IMSI-catchers during political protests to identify, track, and intercept the communications of protestors, journalists, and opposition groups in order to target, censor, and/or arrest them. In order to protect citizens from this repressive surveillance, OTF has supported the development of tools to detect the use of IMSI-catchers based on research conducted by the University of Washington and has piloted this technology in three Latin American cities.

### Combatting Internet Shutdowns

Over the last year, governments around the world have shut down the internet over 188 times. In order to ensure that citizens can continue to access and share digital content in the face of internet shutdowns, OTF has invested in unique peer-to-peer technologies that enable content-sharing and communication without an internet or cellular connection. For example, OTF has supported the development of **Briar**, an open- source, decentralized, encrypted messaging system that is designed for journalists, human rights defenders, and anyone who needs a safe and easy way to communicate when internet connectivity is uncertain. OTF has incubated **F-Droid**, an alternative app store for Android that allows users to easily share apps with others in their vicinity without an internet connection. In addition, OTF has supported the development of Ouinet. **Ouinet** is a free, open source technology, which allows web content to be served with the help of an entire network of cooperating nodes using peer-to-peer routing and distributed caching of responses.

**Timely, Accurate Censorship Detection**
Growing levels of internet censorship has heightened the need for robust censorship detection and analysis tools. Without knowledge of what is being blocked where and the underlying technical means for doing so, it is very difficult for circumvention tool developers to understand their adversaries' capabilities and to create effective tools to respond. Recognizing this, OTF has invested in the development and implementation of leading censorship detection tools, including the Open Observatory of Network Interference (OONI) and the Internet Outage Detection and Analysis (IODA) project. OONI is an open-source networking testing framework and testing network for detecting network interference including outright censorship. IODA is a system that monitors the internet in near-real time to identify macroscopic internet outages affecting the edge of the network. Collectively, these projects measure and document internet censorship nearly every minute in more than 210 countries.

**Exposing Repressive PRC Surveillance**
OTF has also played a key role in investigating and exposing PRC-affiliated apps used for repressive surveillance, including tools used by the government to target religious minority Uyghur Muslims in Xinjiang province as well as the widely used PRC-affiliated app, Study the Great Nation. In addition to exposing the increasingly sophisticated tactics that the Chinese government is using to surveil and control their own citizens, this research has also helped to shine a light on the types of technologies and tactics that the Chinese government is exporting to like-minded regimes around the world.

OTF conducted an audit of the **"BXAQ" app** that is used by Chinese police in the Xinjiang province to scan tourists' mobile phones. The audit found that the app not only scans phones but also captures users' data and sends that information insecurely to a local file server for analysis. In conjunction with Human Rights Watch, OTF also supported technical researchers to analyze a data collection and analysis system, called the **Integrated Joint Operations Platform (IJOP)**, that is used by police in the Xinjiang region to track residents. Researchers found that the system tracks the location data of phones, ID cards, and vehicles as well as the use of electricity and gas stations by all residents in the region. When the IJOP system detects irregularities or deviations from the norm, the system flags these abnormalities to authorities as suspicious, which prompts an investigation. In addition, OTF supported research on the mobile application, known as **Jingwang**, that all residents of Xinjiang have been forced to install on their mobile phones. Researchers found that the app collects personally identifiable information, scans the device for "dangerous" files, and sends a list of all files to an unknown entity for monitoring. Research supported by OTF also tracked the export of Chinese censorship and surveillance technologies and tactics to **102 countries** around the world.

**Responding to Digital Emergencies around the World**
Over the last year, OTF supported rapid response interventions across the globe to help journalists and human rights defenders respond to digital attacks and other forms of online censorship, including in places such as Venezuela, Hong Kong, Iran, Egypt, Gambia, DRC, Tibet, Thailand, Bahrain, Sudan, Ethiopia, Pakistan, Vietnam and Azerbaijan.

- **Venezuela:** After Venezuela's contested 2018 presidential election, the Maduro regime drastically ramped up its internet censorship and online attacks against journalists and activists. These attacks escalated further in 2019 with authorities regularly implementing "just-in-time" censorship tactics to block media content and popular social platforms. In response to this worsening censorship environment, OTF quickly activated its networks to detect and monitor new censorship events, provide rapid response digital security assistance to journalists and activists on the ground, and deploy anti-censorship and secure communication tools for tens of thousands of citizens. OTF also provided rapid response assistance to a leading Venezuelan human rights organization and a network of Venezuelan journalists that were the targets of government-sponsored hacking attempts. These combined efforts ensured that activists and journalists were able to continue safely communicating and reporting on the situation.

- **Hong Kong:** In late 2019, protests erupted in Hong Kong in opposition to a proposed extradition law that would essentially subject its citizens to the Chinese legal system. Shortly after the protests began, Hong Kong-based journalists and human rights organizations reached out to OTF for digital security support and assistance. In response, OTF supported the creation of a tailored Chinese/English digital security guide for journalists and protesters, quickly deployed anti-censorship and secure communications tools to over 100,000 citizens, and supported the integration of OTF-incubated New Node into the popular Telegram app to improve the security and resiliency of communications.

- **Iran:** OTF responded quickly to the internet shutdown in Iran in November 2019. OTF-supported network measurement tools, including OONI and IODA, immediately reported the shutdown and closely monitored the situation in Iran. OTF collected this information in real-time and shared it with circumvention tool developers in order to help them update their tools accordingly and integrate new, effective circumvention techniques. OTF also shared this information with USAGM news networks to improve reporting and raise awareness about the technical aspects of the shutdown. In addition, OTF worked with the USAGM networks, the State Department, and Iranian human rights organizations to distribute the OTF-incubated Briar and F-Droid app to journalists, protestors, and civil society in Iran to enable peer-to-peer messaging during the shutdown so that users could continue to communicate and share information.

## CONCLUSION

The technologies funded by OTF over the last year have played a critical role in advancing the state of the art of anti-censorship and secure communication technologies globally. However, threats to internet freedom continue to grow exponentially as repressive regimes deploy increasingly bold and sophisticated censorship and surveillance tactics and technology. Over the last year, regimes have started to deploy artificial intelligence (AI) and machine learning to enable faster, more targeted, and more aggressive online censorship and surveillance. These new technologies have significantly decreased the cost of mass censorship and surveillance, making these tactics and techniques easily accessible to repressive regimes around the world. In many countries, repressive regimes have also begun to deploy new and nefarious technologies to create and propagate disinformation. By combining advanced censorship and surveillance technology with disinformation tactics, repressive regimes are now able to control and manipulate the online information landscape in a way they never have before. In addition to advanced and nefarious technical approaches, repressive regimes have become bolder and more aggressive in their online

censorship tactics, going so far as to cut their citizens off from the internet entirely. Over the last year, governments around the world shut down the internet over 188 times, including in Iraq and Iran. On average, internet shutdown cost countries over $20 million per day in GDP, demonstrating just how far repressive regimes will go to stop the free flow of information.
As threats to internet freedom continue to increase globally, so too have the need and demand for internet freedom projects. As a leading internet freedom funder and trusted partner among the global technical and human rights communities, requests for support from OTF have also grown exponentially. Over the last seven years, OTF has reviewed and responded to nearly 5,000 requests for support seeking over $500 million in total. In just the last year, OTF reviewed and responded to over 1,400 requests for support.

Building on years of success and impact in promoting and enabling the unrestricted use of the internet in places where internet freedom is attacked, OTF is poised to greatly expand effectiveness through a transition to a more streamlined, mature and dynamic organization. This new structure will enable OTF to support more strategic, coordinated, and resilient internet freedom programs to combat increasingly sophisticated and widespread online censorship and repressive surveillance as we move into FY 2020 and beyond.